Matt Zagame

Dr. Haim Levkowitz

Mobile App Programming II

March 2, 2022

The Future of Blockchain

Abstract

Blockchain has been one of the fastest growing technologies to emerge in the digital age. The interest in blockchain technology stems from its ability to cryptographically store information on a decentralized immutable database. The most common implementation of blockchain being a distributed ledger system which is used by cryptocurrencies to securely record transactions without the need for an intermediary. As it stands, blockchain has already proven to have a multitude of valuable use cases. The purpose of this paper is to analyze how blockchain is currently being implemented in order to determine a broad perspective on what the future could look like for blockchain and the implications it would have on existing technologies such as the Internet and payments. An analysis of current implementations is presented along with a discussion of key principles and innovations that make blockchain a disruptive technology. The results show that blockchain has laid the groundwork for a wide variety of real-world applications, however there are several areas for improvement that should be further developed before it can experience mass adoption.

Introduction

Over the past few years, blockchain has gained a lot of attention. This can be largely attributed to the success of cryptocurrencies such as Bitcoin which are built upon blockchain technology. The reason blockchain has been able to maintain its momentum is due to the fact that the technology offers a number of solutions to existing problems and inefficiencies in the financial and digital world today. The most prominent feature being the decentralization of data.

In layman's terms, a blockchain is a type of append-only data structure that uses cryptography to chain blocks of data together. In the case of cryptocurrency, blockchain is used as a distributed ledger system that keeps a record of every transaction that takes place on the network. This provides a more secure and verifiable method of transacting than in traditional financial systems which would require a certain degree of trust on a third party to complete a transaction. The decentralized nature of blockchains also means that a user’s data cannot be accessed by any other entity without their permission, making it a secure digital database.

In recent years, slightly more modern blockchains have also begun to explore new features such as smart contracts and decentralized applications. Additionally, many financial and academic institutions have started to delve into the underlying architecture of blockchain to try to better understand the technology. Given the benefits that blockchains present today, and the increased demand for blockchains that boast high-performance and innovative features, it is clear that this technology has a promising future. As such, an in-depth analysis should serve to clear up any doubts about the future of blockchain.

Blockchain Implementation

In late 2008, pseudonym Satoshi Nakamoto published the whitepaper for Bitcoin which detailed a peer-to-peer electronic cash system that focused on removing the need for a trusted third-party while transacting online. Bitcoin proposed to solve digital commerce along with the double-spending problem by introducing the world's first successful implementation of blockchain. The Bitcoin blockchain is maintained by a proof-of-work consensus mechanism which requires various nodes operating the network to agree on the validity of transactions. This is done by solving a difficult computational proof-of-work for every block, also known as mining. Once a node finds a proof-of-work, it broadcasts the block to every other node and that block is added onto the chain so long as the transactions are valid and not already spent. Nodes are then rewarded with Bitcoin for the confirmation of blocks as an incentive to run the network. In addition, chaining transactions by signing a hash of each previous transaction with the current transaction's public key ensures authentic ownership of transacted coins. Depending on the issuance of the nodes running the network, a problematic scenario for Bitcoin could arise. If more than fifty percent of the network's nodes are under control of a central authority, this authority would be able to propagate a dishonest chain, allowing manipulation of transactions.

In most cases, more recent blockchains are built in a way that is not too dissimilar to Bitcoin. Many alternative cryptocurrencies use different block sizes and unique consensus mechanisms. For instance, cryptocurrencies with smaller block sizes may offer faster block confirmation times, but are typically less secure. The purpose for different consensus mechanisms is often to mitigate the amount of computational power that is necessary to run the chain (Catalini and Gans 2020). An example of this is another common form of consensus known as proof-of-stake.

Ethereum, the second largest cryptocurrency by market capitalization, is currently undergoing a series of network upgrades that will transform its consensus from proof-of-work to proof-of-stake. Proof-of-stake allows users to stake their cryptocurrency on-chain via smart contracts in order to maintain the network. The more cryptocurrency a user has staked, the greater their chances are of creating a new block and therefore the more rewards are paid out to the stakeholder (BitFury Group 2015). This incentivizes users who believe in the network to stake more of the cryptocurrency to not only be rewarded more so than others, but also to better secure the network as well. In order for an attacker to successfully disrupt this type of network, they would need to own a majority of the supply of the cryptocurrency. Assuming that the cryptocurrency is of any value, this is by design very unlikely to ever happen.

Another innovation in the blockchain space that has gained traction is the introduction of smart contracts. Smart contracts allow users to execute transactions on the network based on one or more conditions. This type of system can be used to set up payments for contractors, and could even replace lawyers and banks that rely on pre-defined conditions for asset deals (Nofer et al. 2017). Smart contracts can also be set up using independent oracles so that assets are managed based on market conditions or conditions from various other data sources (Catalini and Gans 2020). The implementation of smart contracts helps give blockchains more applications in the real world, and also play a large role in decentralized applications. Currently, decentralized applications are capable of facilitating the exchange of digital assets, offering decentralized storage, and letting users vote on network proposals. As the tokenized economy of blockchains continues to grow, decentralized applications may become capable of much more than they are today.

Analysis

Some of the biggest problems with financial markets are due to the reliance on vastly outdated models. Slow and tedious processes such as tracing back ownership in long transaction chains and settlements. As it stands, intermediaries are responsible for carefully and accurately recording transactions so that everything is in proper order. In addition, it can take several days for money to be transferred between banks. Blockchain technology aims to overcome the risks involved in these legacy financial situations by replacing trust in people with trust in mathematical structures (Nofer et al. 2017). Since blockchains do not rely on third parties to verify information, they are inherently more secure and allow for a trustless transaction of information. Blockchain, naturally, could play a large role in the financial sector due to its ledger-like properties being able to work in real-time. In its current state however, blockchain is not without its limitations.

On a fundamental level, blockchains have three primary aspects. These are, decentralization, scalability, and security. The problem lies in the fact that there has yet to be a blockchain that accomplishes all three without sacrificing at least one aspect. This is known as the blockchain trilemma. Bitcoin, for example, has experienced an increase in decentralization given its expanding network effect. However, an increase in network activity brings about scalability concerns. A primary concern for Bitcoin comes with adding a lot of blocks to the network at once which may cause performance problems. Solutions such as the Lightning Network have been proposed to offload some of the transactions using parallel channels which would reduce the amount of blocks on the main ledger tremendously if implemented at scale. Another concern for most involved with cryptocurrency is security. As previously detailed, a controlled concentration of more than fifty percent of the nodes running the Bitcoin blockchain would allow a bad actor to manipulate the transactions on the ledger. Unfortunately for most

blockchains, scalability and decentralization are often held back by security, but security tends to be compromised by protocols focusing on scalability (Ledger 2021). Therefore as of late, much focus on the development of blockchain technology has been to find a solution to the blockchain trilemma.

Discussion and Future Trends

As of the date on this paper, proof-of-work and proof-of-stake are the two most established forms of consensus in blockchain. Each offers a unique set of pros and cons worth discussing in further detail.

Proof-of-work is perhaps best known as the reason why Bitcoin received so much criticism in recent years due to being heavily resource-inefficient. In fact, in 2016 Bitcoin mining was reported to waste $15 million a day (Yli-Huumo et al.). The counter-argument is that Bitcoin is more secure this way, it is much harder to launch an attack when the resources required to do so would be quite costly. This effectively makes Bitcoin a safer store of value, demonstrating that the value proposition for Bitcoin is derived from the energy required to run the network.

On the other hand, proof-of-stake gains value through trust in the protocol. For the network to be maintained, users must lock up their cryptocurrency in smart contracts to stake them. The amount staked is directly related to the creation of new blocks on-chain. Since users with more of the underlying cryptocurrency have more control over the operation of the network, the proof-of-stake system can be argued to be less decentralized than other blockchains. As for now, it would seem that both forms of consensus are far from perfect.

In the future, innovative entrepreneurs who are willing to work with cryptocurrencies could allow blockchain to flourish. Some of the trending implementations of blockchain that are currently being prototyped include the next evolution of the web (web3), decentralized exchanges, self sovereign identity, voting, real estate, digital art, and the list goes on. Each of these innovations either improve upon technologies that still only exist in the physical world or improve upon aspects of the internet, which has become an important part of many people's lives. So long as there is a degree of trust in the technology, the possibilities are endless for blockchain.

Conclusion

As the number of blockchain projects continues to grow and cover more ground, it is difficult to discern exactly which direction the technology is headed. Various applications of blockchain are possible and actively being developed. The most common implementation being cryptocurrency which is largely trying to solve the problem of money transfers. While there are several approaches for reaching consensus on a blockchain, it is clear that these systems still have some drawbacks that need to be worked out before a solid foundation is set. Once a truly decentralized, secure, and scalable solution is found, there is no telling how far blockchain technology will go.

References

Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf.

BitFury Group. *Pos vs Pow 1.0.2 - Bitfury*. 23 Sept. 2015, https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf.

Catalini, Christian and Joshua S. Gans. "Some simple economics of the blockchain." Communications of the ACM 63, 7 (June 2020): dx.doi.org/10.1145/3359552. © 2020 Owner/Author

“What Is the Blockchain Trilemma?” *Ledger*, 15 Nov. 2021, https://www.ledger.com/academy/what-is-the-blockchain-trilemma.

Nofer, Michael, et al. “Blockchain - Business & Information Systems Engineering.” *SpringerLink*, Springer Fachmedien Wiesbaden, 20 Mar. 2017, https://link.springer.com/article/10.1007/s12599-017-0467-3.

Yli-Huumo, Jesse, et al. “Where Is Current Research on Blockchain Technology?-a Systematic Review.” *PLOS ONE*, Public Library of Science, https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163477.